KOMTELKA: Jurnal Komputer Telekomunikasi dan Elektronika, Volume 01 Nomor 1 Tahun 2026
Tersedia *online* di
https://jurnal.rajawalicemerlangabadi.com/index.php/jpek

Permasalahan Cybercrime dalam Perkembangan Teknologi Blockchain dan Cloud Computing di Indonesia

Irma Lestari[1], Gita Lestarini Rahayu[2], Yuliarman Saragih[3]

[1,2,3]*Universitas Singaperbangsa Karawang*

email: [1]2510631010022@student.unsika.ac.id, [2]2510631010126@student.unsika.ac.id, [3]yuliarman@yahoo.com

Kata kunci:
Kejahatan Siber
Blockchain
Komputasi Awan
Keamanan Siber
Indonesia

Keywords:
Cybercrime
Blockchain
Cloud Computing
Cybersecurity
Indonesia

ABSTRAK

Transformasi digital mendorong organisasi memanfaatkan teknologi seperti cloud computing, blockchain, big data, Internet of Things, dan kecerdasan buatan untuk meningkatkan efisiensi serta kualitas layanan. Namun, perkembangan teknologi juga memunculkan ancaman cybercrime berupa phishing, ransomware, pencurian identitas, dan pelanggaran data yang merugikan individu, perusahaan, maupun negara. Blockchain menawarkan keamanan melalui sistem desentralisasi dan validasi kriptografi yang sulit dimanipulasi, sedangkan cloud computing memerlukan perlindungan data yang kuat agar terhindar dari serangan siber. Di Indonesia, penanggulangan cybercrime dilakukan melalui Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi. Penegakan hukum melibatkan berbagai lembaga untuk memperkuat keamanan siber nasional dan meningkatkan kepercayaan masyarakat terhadap sistem digital. Selain itu, edukasi masyarakat mengenai keamanan digital diperlukan untuk mencegah penyalahgunaan data dan meningkatkan kewaspadaan siber nasional.

ABSTRACT

Digital transformation encourages organizations to utilize technologies such as cloud computing, blockchain, big data, the Internet of Things, and artificial intelligence to improve efficiency and service quality. However, technological developments also give rise to cybercrime threats such as phishing, ransomware, identity theft, and data breaches that harm individuals, companies, and countries. Blockchain offers security through a decentralized system and cryptographic validation that is difficult to manipulate, while cloud computing requires strong data protection to avoid cyberattacks. In Indonesia, cybercrime prevention is implemented through the Electronic Information and Transactions Law and the Personal Data Protection Law. Law enforcement involves various institutions to strengthen national cybersecurity and increase public trust in digital systems. Furthermore, public education about digital security is needed to prevent data misuse and increase national cyber awareness.

PENDAHULUAN

Transformasi digital adalah proses di mana organisasi dan perusahaan mengadopsi teknologi digital untuk secara mendasar mengubah cara mereka berinteraksi dengan konsumen serta menjalankan kegiatan bisnis. Tujuannya adalah

untuk mencapai sasaran strategis dan meningkatkan performa. Proses ini bertujuan untuk menyegarkan cara kerja perusahaan dan komunikasi dengan pelanggan dengan mengaplikasikan teknologi seperti cloud computing, analitik data besar, Internet of Things (IoT), dan kecerdasan buatan, serta untuk meningkatkan kinerja di tengah perubahan cepat era digital. Transformasi digital meliputi penyesuaian proses bisnis terhadap teknologi terbaru dan mempercepat inovasi. Dalam implementasinya, transformasi digital memerlukan dukungan teknologi yang dapat meningkatkan efisiensi, fleksibilitas, dan aksesibilitas terhadap berbagai layanan informasi. Salah satu teknologi yang populer digunakan untuk memenuhi kebutuhan ini adalah cloud computing.[1]

Cloud Computing adalah layanan di bidang teknologi informasi yang memberikan kemampuan kepada pengguna untuk menyimpan serta mengakses data secara daring. Fleksibilitas dan kemudahannya membuat cloud computing sangat populer di kalangan perusahaan maupun individu. Namun, terdapat juga risiko dalam penggunaan cloud computing, termasuk kehilangan data, gangguan pada layanan, isu kompatibilitas aplikasi, dan ancaman dari serangan siber. Sebab itu, penting untuk melakukan upaya pencegahan seperti menerapkan sistem keamanan yang kuat, melakukan pencadangan data secara teratur, melaksanakan pengawasan yang berkelanjutan, serta menyusun rencana untuk pemulihan bencana. Penegakan keamanan digital yang efektif adalah kunci agar kemajuan teknologi dapat memberikan kontribusi positif di berbagai aspek kehidupan.[2]

Perkembangan pesat dalam teknologi digital memberikan dampak positif dalam hal akses informasi, partisipasi sosial, dan peningkatan ekonomi komunitas. Namun, terdapat juga risiko yang mengemuka terkait dengan penyebaran informasi yang salah dan ketergantungan terhadap perangkat digital. Kemajuan teknologi digital telah secara signifikan meningkatkan risiko kejahatan dunia maya, seperti serangan malware, peretasan, dan pencurian data pribadi. Tindak kejahatan ini dapat berakibat pada pencurian identitas, kehilangan pekerjaan, serta gangguan pada infrastruktur penting. Secara umum, masyarakat kurang menyadari ancaman yang ditimbulkan oleh kejahatan dunia maya dan tidak mengetahui cara yang efektif untuk melindungi diri mereka. Hukum serta peraturan terkait kejahatan dunia maya tetap fluktuatif dan sering mengalami perubahan. Sementara itu, pelaku kejahatan

siber terus mengembangkan teknik dan pendekatan baru. Situasi ini menggambarkan bahwa perkembangan kejahatan dunia maya semakin kompleks untuk diatasi dan dapat membawa konsekuensi negatif di berbagai bidang kehidupan.[3]

Bagi masyarakat, kejahatan siber dapat mengakibatkan kerugian finansial, pencurian informasi pribadi, dan berkurangnya rasa aman saat mengakses layanan digital. Bagi perusahaan, serangan jaringan dapat mengganggu kegiatan bisnis, merusak citra perusahaan, serta menimbulkan kerugian finansial yang signifikan sebagai akibat dari kebocoran informasi dan gangguan sistem. Sementara itu, bagi negara, tindakan criminal di dunia maya dapat mengancam stabilitas keamanan nasional, menghalangi perkembangan ekonomi digital, serta menurunkan kepercayaan masyarakat terhadap sistem digital pemerintah. Oleh sebab itu, diperlukan langkahlangkah perlindungan yang lebih efektif dengan menerapkan sistem keamanan data yang kuat dan dapat dipercaya dalam berbagai layanan digital, yang memuat aturan perbaikan, pengujian secara berkala, dan perbaikan instan saat timbul kondisi genting.[4]

Kehadiran sistem keamanan data yang efektif tidak hanya merupakan kebutuhan teknis, tetapi juga merupakan elemen penting dalam menjaga stabilitas, kepercayaan masyarakat, dan kedaulatan digital suatu bangsa. Pengamanan data harus mencakup beberapa hal, baik yang bersifat teknis seperti implementasi firewall, enkripsi, dan sistem deteksi intrusi, serta yang bersifat non-teknis seperti kebijakan pengelolaan data, regulasi hukum, dan pelatihan untuk SDM. Di samping penerapan elemen teknis dan non-teknis, perlindungan data juga harus diperkuat dengan hukum yang jelas dan sesuai dengan kemajuan teknologi digital. Yakni, Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi menjadi langkah krusial di sistem hukum di Indonesia yang dengan khusus mengatur perlindungan data diri di era digital. Undang-undang ini muncul sebagai reaksi terhadap peningkatan kasus penyalahgunaan dan kebocoran data yang sebelumnya tidak memiliki dasar hukum yang kuat. Sebelumnya, perlindungan data pribadi hanya diatur secara terbatas dalam berbagai peraturan sektoral, seperti UU ITE, UU Kesehatan, serta UU Perbankan, yang belum mampu secara komprehensif

melawan hambatan perlindungan data dalam ranah digital yang rumit dan terus berubah.[5]

Berdasarkan hal tersebut, rumusan masalah dalam penelitian ini adalah apa saja bentuk cybercrime yang muncul dalam penggunaan blockchain dan cloud computing serta bagaimana upaya hukum dan keamanan siber dalam mengatasi cybercrime di Indonesia, dengan tujuan untuk mengetahui bentuk-bentuk cybercrime dalam penggunaan blockchain dan cloud computing serta menganalisis upaya hukum dan keamanan siber dalam penanggulangan cybercrime di Indonesia.

METODE PENELITIAN

Penelitian tentang Isu Cybercrime dalam Evolusi Teknologi Blockchain dan Cloud Computing di Indonesia menerapkan pendekatan penelitian kualitatif yang bersifat deskriptif. Cara ini diterapkan untuk menjelaskan dan mengevaluasi berbagai jenis cybercrime yang muncul seiring dengan kemajuan teknologi digital di Indonesia, terkhusus dalam teknologi blockchain dan cloud computing.

Pendekatan yang dipilih dalam studi ini meliputi pendekatan yuridis normatif serta pendekatan teknologi informasi. Pendekatan yuridis normatif ditujukan untuk meneliti regulasi dan hukum yang terkait dengan cybercrime, sedangkan pendekatan teknologi informasi berfungsi untuk memahami perkembangan blockchain, cloud computing, serta ancaman terhadap keamanan digital yang muncul.

Dalam kajian mengenai Isu Kejahatan Siber dalam Evolusi Teknologi Blockchain dan Cloud Computing di Indonesia, alat penelitian digunakan untuk mendukung proses pengumpulan informasi, pemrosesan data, analisis studi, serta penyusunan hasil publikasi. Penggunaan alat tersebut bertujuan agar proses penelitian dapat dilaksanakan dengan lebih terstruktur, efisien, dan didukung oleh data yang relevan. Jenis alat yang digunakan dalam kajian ini mencakup:

A. Alat Pengumpulan Data

Alat ini dipakai untuk mengumpulkan informasi dan referensi terkait dengan kejahatan siber, blockchain, dan cloud computing, antara lain:

1. Studi literatur
2. Jurnal baik lokal maupun internasional
3. Artikel penelitian
4. Situs resmi pemerintah
5. Google Scholar

B. Alat Pengolahan dan Penyusunan Data

Alat ini dimanfaatkan untuk mendukung proses penyusunan dan pengelolaan data penelitian, termasuk:

1. Microsoft Word untuk penulisan laporan penelitian
2. Mendeley atau Zotero untuk pengelolaan referensi dan sitasi

C. Alat Keamanan Jaringan

Dalam studi ini, beberapa alat keamanan jaringan juga diterapkan sebagai bagian dari diskusi mengenai kejahatan dunia maya, yang meliputi:

1. Perimeter keamanan
2. Perangkat lunak pencegah virus dan malware
3. Autentikasi multi-faktor (MFA)
4. Perangkat enkripsi

Alat-alat ini dimanfaatkan untuk mendukung perlindungan terhadap sistem digital serta mengurangi kemungkinan terjadinya kejahatan siber.

D. Alat Blockchain

Penelitian ini menerapkan berbagai alat blockchain untuk mendalami tindakan serta aspek keamanan dalam teknologi blockchain, seperti:

1. Penjelajah blockchain
2. Platform smart contract
3. Analisis cryptocurrency

Alat-alat ini digunakan untuk mengevaluasi transaksi digital dan mengidentifikasi potensi ancaman kejahatan siber pada jaringan blockchain.

E. Sumber Referensi Penelitian

Sumber referensi dalam penelitian ini berguna untuk memperkuat analisis dan diskusi yang dilakukan, mencakup:

1. Buku tentang keamanan siber
2. Jurnal yang membahas kejahatan siber

3. Regulasi yang diterbitkan oleh pemerintah
4. Laporan dari Badan Siber dan Sandi Negara (BSSN)
5. Artikel yang membahas blockchain dan cloud computing

Dengan memanfaatkan alat dan sumber referensi tersebut, penelitian ini diharapkan dapat memberi analisis yang lebih mendalam terkait isu kejahatan siber dalam perkembangan teknologi blockchain dan komputasi awan di Indonesia.

PEMBAHASAN

A. Bentuk Cybercrime Yang Muncul Dalam Penggunaan Blockchain Dan Cloud Computing

Perkembangan ekonomi berbasis digital menghasilkan kemudahan serta menghadirkan risiko yang baru. Peningkatan frekuensi transaksi secara elektronik telah menyebabkan lonjakan insiden kejahatan siber, seperti phishing, ransomware, pencurian identitas, dan pelanggaran data. Metode yang digunakan oleh para penjahat semakin kompleks, termasuk dalam hal pemalsuan data digital dan penyebaran perangkat lunak jahat serta penggunaan sistem keuangan yang curang di dunia maya. Sistem keamanan yang sudah ada yang bergantung pada kekuasaan pusat sangat rentan, karena satu titik lemah saja bisa menyebabkan kebocoran data yang signifikan. Teknologi blockchain memperkenalkan cara baru untuk mengamankan melalui kesepakatan gabungan dan validasi berbasis kriptografi. Per-transaksi dalam koneksi blockchain memerlukan persetujuan dari sebagian besar node dengan cara-cara semacam Proof of Work (POW) dan Proof of Stake (POS). Ini membuat manipulasi informasi menjadi hampir tidak mungkin. Untuk mengubah satu blok, seseorang yang berniat jahat harus mendapatkan persetujuan dari lebih dari setengah node jaringan secara bersamaan, yang merupakan tugas yang sangat sulit dari segi teknis dan biaya. Selain itu, adanya kontrak pintar yaitu program otomatis yang berjalan berdasarkan syarat yang telah ditentukan sebelumnya yaitu menurunkan kemungkinan adanya campur tangan manusia. Dalam konteks transaksi digital, smart

contract menjamin bahwa kesepakatan dapat berjalan secara otomatis tanpa melibatkan pihak ketiga.[6]

Bentuk cybercrime yang pertama adalah phishing, yang merupakan salah satu bentuk serangan dunia maya yang melibatkan usaha penipuan atau forgery untuk memperoleh informasi sensitif, seperti password, informasi kartu kredit dan data pribadi lainnya dari orang-orang yang tiada menyadari bahaya. Taktik ini dilakukan melalui berbagai media, seperti surel, pesan melalui SMS, dan laman web. yang menyerupai aslinya. Beberapa contoh risiko phishing termasuk: Email Phishing, Spear Phishing, dan Pharming, para pelaku penipuan menuntun arus jaringan korban menuju server yang tidak asli guna mengambil informasi seperti kode akses. Serangan phishing dapat mengakibatkan kerugian baik dari segi keuangan maupun reputasi yang besar bagi perusahaan dan pada akhirnya merusak kepercayaan pengguna.[7]

Selanjutnya, kita akan membicarakan mengenai ransomware. Ransomware adalah jenis program riskan yang dibuat guna mengenkripsi data atau sistem komputer milik orang lain, atau untuk mencegah akses ke dalamnya. Para pelaku kejahatan yang memanfaatkan ransomware meminta imbalan berwujud mata uang kripto guna mengembalikan informasi atau sistem kepada pemilik aslinya.[8]

Salah satu jenis kejahatan yang semakin meningkat di dunia maya adalah pencurian identitas. Dalam pengertian, pencurian identitas berhubungan dengan perolehan, penguasaan, atau pemanfaatan data identitas seseorang secara tidak sah demi maksud tertentu. Pada implementasinya, pelanggar mendayagunakan informasi terkait guna mendapatkan akses ke layanan finansial, menciptakan pengguna palsu, mengusulkan pinjaman secara online, sampai melaksanakan transaksi yang tidak legal mewakili nama korban. Sebagai resikonya, korban mengalami bukan hanya kerugian finansial karena kehilangan harta dan peningkatan utang, tetapi juga kerugian nonfinansial yang meliputi kerusakan reputasi, tekanan mental, dan berkurangnya kepercayaan terhadap sistem digital.[9]

Yang terakhir adalah pelanggaran data, yaitu sebuah kejadian di mana informasi pribadi atau data penting lainnya diakses, disampaikan, atau dicuri oleh individu yang tidak memiliki izin. Dalam ranah siber, kejadian ini umumnya terjadi akibat serangan siber, kebocoran sistem, atau kelalaian dari pihak yang mengelola data.[10]

B. Upaya Hukum Dan Keamanan Siber Dalam Mengatasi Cybercrime Di Indonesia

Kejahatan siber adalah jenis kejahatan yang muncul dalam era modern, sejalan dengan perkembangan teknologi informasi. Tindak pidana ini sangat terkait dengan penggunaan komputer. Kejahatan siber mampu mengancam kerahasiaan, integritas, dan keberadaan data baik individu maupun negara. Kejahatan siber memerlukan pengawasan yang ketat dari pihak pemerintah karena perbedaannya yang jelas dengan kejahatan konvensional. Kejahatan siber terjadi secara luas dan merugikan banyak orang. Di Indonesia, kejahatan siber diatur oleh Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Aturan tersebut mencakup berbagai model transaksi dan kegiatan yang dilangsungkan melalui cara digital, meliputi pemencaran konten tidak sah, penipuan online, pembajakan data, dan pembobolan. Terutama di Indonesia, di mana kejahatan siber semakin meningkat, pemerintah menaruh perhatian pada penerapan hukum yang cepat untuk bisa memberikan sanksi kepada para pelaku.

Pemerintah Indonesia telah mengatur perihal kejahatan siber dalam UndangUndang Teknologi Informasi dan Komunikasi untuk menghentikan, mengurangi, serta mencegah tindakan kriminal di dunia digital. Peraturan ini mencakup berbagai jenis kejahatan siber, berawal dari tersebarnya konten yang dilarang sampai penipuan serta pembobolan. Menjadi reaksi tentang naiknya kejahatan siber yang berkaitan dengan manipulasi identitas, UU No. 27 Tahun 2022, telah diresmikan. Hukum ini menekankan bahwa pengamanan data individu adalah otoritas yang dilindungi oleh konstitusi dan harus dihormati, serta menyediakan rancangan regulasi yang ketat lewat

pendirian Badan Perlindungan Data Pribadi, sebuah lembaga untuk pemantauan ketatausahaan, dan nestapa yang ketat. Penyimpangan seperti pengumpulan, distribusi, dan perubahan data pribadi tanpa izin dapat mengakibatkan hukuman penjara dan/atau denda yang sangat besar, ditambah dengan sanksi lainnya seperti kompensasi untuk para korban.

Kejahatan digital di negara kita dikoordinasikan oleh UU ITE, yang memberikan definisi mengenai kejahatan siber dan menjelaskan secara lebih rinci dalam Pasal :

1. Pasal 29 UU ITE: Mengatur mengenai ancaman kekerasan melalui media elektronik, seperti penyampaian informasi elektronik atau dokumen elektronik yang berisikan ancaman kekerasan atau intimidasisecara pribadi.

2. Pasal 30 jo. Pasal 34 UU ITE: Mengatur mengenai perbuatan kejahatan, misalnya menghasilkan, memasarkan, mendatangkan barang dari luar negeri, mengedarkan, mengadakan, atau mempunyai perangkat keras.

3. Pasal 46 UU ITE: Menjelaskan mengenai pencurian dalam konteks kejahatan siber.

4. Pasal 34 ayat (1) jo. Pasal 50 UU ITE: Menjelaskan mengenai pencurian dengan kolaborasi dalam kasus siber.

5. Pasal 35 Jo Pasal 51 ayat (1) atau Pasal 32. Pasal 48 UU ITE: Menjelaskan mengenai penipuan dalam konteks siber, terutama lewat pengumpulan informasi kartu kredit dan transaksi daring.

Karena kriminalitas dunia maya bisa terjadi di mana saja, hal ini memerlukan tanggapan yang tegas dan perhatian penuh dari pemerintah. Pendekatan Indonesia terhadap keamanan dunia maya dan penegakan hukum dimulai dengan penyelarasan peraturan untuk mencakup seluruh aspek kejahatan siber dalam kerangka hukum yang lengkap. Pemerintah sedang berusaha untuk menyelaraskan

Undang-Undang Ketahanan Siber dengan UU ITE, UU PDP, dan bermacam aturan khusus lain. Langkah ini tidak hanya akan memperjelas pengertian dari kegiatan siber yang ilegal, tetapi juga memastikan adanya prosedur pelaporan dan penyelidikan yang terstruktur, serta berbagai hukuman, termasuk denda administratif dan pidana, tanpa adanya celah dalam yurisdiksi. Harapan dari upaya ini adalah untuk mengurangi risiko adanya tumpuan kekuasaan antar institusi dan memungkinkan penanganan serangan siber dengan cepat, hingga kebijakan nasional dapat segera merespons perubahan teknologi yang berlangsung cepat.

Di Indonesia, berbagai lembaga, termasuk Polri, Kejaksaan Agung, dan KPK, berperan dalam memberantas aktivitas siber yang melanggar hukum. Polri memiliki tim khusus yang ditugaskan untuk menyelidiki kejahatan siber, seperti Unit Penyidikan Kejahatan Siber Bareskrim Polri. Dan juga, peran Kejagung sangat signifikan dalam menuntut para pelaku kejahatan siber. Tantangan lain dalam pengembangan kebijakan keamanan siber adalah sifat dari ancaman yang bersifat multidimensi. Hal ini menyebabkan upaya penanganan tidak hanya menjadi tanggung jawab Tentara Negara Indonesia ataupun Polisi RI, tetapi juga mengikutsertakan kementerian lainnya seperti Kemhan serta KemKominfo.

KESIMPULAN

Kemajuan dalam teknologi digital, terutama blockchain dan cloud computing, telah memberikan sejumlah keuntungan bagi masyarakat dan sektor bisnis di Indonesia, seperti kemudahan dalam bertransaksi, efisiensi dalam penyimpanan informasi, serta peningkatan konektivitas. Namun, di sisi lain, kemajuan ini juga menghadirkan berbagai jenis kejahatan siber yang semakin rumit, termasuk phishing, ransomware, pencurian identitas, dan pelanggaran data. Tindak kriminal ini memanfaatkan kelemahan dalam sistem keamanan, rendahnya tingkat kesadaran pengguna, dan celah dalam pengelolaan data digital.

Teknologi blockchain menyediakan solusi keamanan yang lebih handal melalui sistem yang terdesentralisasi, validasi dengan kriptografi, dan smart contract yang dapat mengurangi risiko manipulasi data serta ketergantungan pada pihak ketiga. Walaupun demikian, teknologi ini tidak sepenuhnya menghilangkan risiko

siber karena faktor manusia dan kelemahan dalam penerapan sistem masih dapat dimanfaatkan oleh pelaku kejahatan.

Di Indonesia, pemerintah telah berusaha mengatasi cybercrime melalui berbagai peraturan, seperti UU ITE serta UU PDP. Selain itu, penegakan hukum dilakukan oleh lembaga terkait seperti Direktorat Tindak Pidana Siber Bareskrim Polri yang didukung oleh kolaborasi antarinstansi. Meskipun demikian, tantangan dalam mengatasi cybercrime tetap cukup signifikan karena sifat kejahatan siber yang bersifat lintas negara, pertumbuhan yang cepat, dan memerlukan kemampuan teknologi yang canggih.

DAFTAR PUSTAKA

[1]. N. Nurasyifa, F. Assyifaurrohmah, and D. Wahid, "Strategi Keamanan Data di Era Transformasi Digital : Tantangan Cloud Computing , Internet of Things , dan Blockchain," vol. 13, no. 2, pp. 200–213, 2025.

[2]. R. D. Hapsari and K. G. Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," *J. Konstituen*, vol. 5, no. 1, pp. 1–17, 2023, doi: 10.33701/jk.v5i1.3208.

[3]. T. W. E. Suryawijaya, "Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia," *J. Stud. Kebijak. Publik*, vol. 2, no. 1, pp. 55–67, 2023.

[4]. F. M. 2025 Ramli, Muzakir, "Jebital : Jurnal Ekonomi dan Bisnis Digital," vol. 2, no. September, pp. 64–73, 2025.

[5]. N. Azzahra, A. Aulia, A. Firmansyah, and A. U. Hosnah, "Pemanfaatan Blockchain Dalam Pencegahan Cybercrime Pada Transaksi Digital," pp. 3169–3175, 2025, [Online]. Available: https://www.jagoanhosting.com/blog/node-adalah/

[6]. B. Wibowo and T. Hidayat, "Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ," *J. Pengabdi. Masy. Sultan Indones.*, vol. 2, no. 1, pp. 1–9, 2024, doi: 10.58291/abdisultan.v2i1.294.

[7]. A. Suciara, D. Michelin, G. A. Loway, G. Amaze, M. A. Fathoni, and M. L. Lediana, "Pencurian Identitas Digital sebagai Bentuk Kejahatan Pendahuluan dalam Cybercrime," pp. 5373–5387, 2026.

[8]. R. S. Silalahi, "Analisis Hukum Tindak Pidana Cyber Data Breach Di Era Digital Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik (Studi Putusan Nomor 2447/Pid.Sus/2024/Pn Mdn)," vol. 4, no. 9, pp. 2425–2440, 2025.

[9]. U. I. N. Sunan and K. Yogyakarta, "Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia Rahma Agri Firdaus Pendahuluan Hukum pidana siber adalah cabang dari hukum pidana yang khusus mengatur tentang tindak pidana yang dilakukan dengan menggunakan," vol. 4, no. 1, 2024.

[10]. B. Hartono, "Ransomware: Memahami Ancaman Keamanan Digital," *Bincang Sains dan Teknol.*, vol. 2, no. 02, pp. 55–62, 2023, doi: 10.56741/bst.v2i02.353.